9-2017

Personal Data Protection Act 2012: Understanding the consent obligation

Man YIP
Singapore Management University, manyip@smu.edu.sg

PERSONAL DATA PROTECTION ACT 2012: UNDERSTANDING THE CONSENT OBLIGATION*

YIP Man†
LLB (Hons) (National University of Singapore), BCL (Oxford); Advocate and Solicitor (Singapore)

I. Introduction

1 The Personal Data Protection Act 2012[1] ("PDPA") provides the baseline standards of protection of personal data and works in tandem with existing law to provide comprehensive protection. The birth of the legislation clearly signals Singapore's commitment to protect the collection, use and disclosure of personal data in the age of big data and its awareness of the importance of such protection in strengthening Singapore's position as a leading commercial hub. Significantly, the PDPA protection model balances "both the rights of individuals to protect their personal data" against "the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes".[2] The approach is thus a pragmatic one. The legislation does not promise uncurtailed protection of informational privacy of the individual, a model that would be practically difficult to

---

* Any views expressed in this article are the author's personal views only and should not be taken to represent the views of her employer. All errors remain the author's own.

† Associate Professor of Law, School of Law, Singapore Management University; DS Lee Foundation Fellow. Yip Man is a Panel Speaker on "Restitution" for the Attorney-General's Chambers' Professional Development Programme, the Asia Pacific Digest Editor for the Restitution Law Review and a co-Administrator of the Singapore Law Blog. She previously served as a member of the Singapore Academy of Law Law Reform Committee.

1 Act 26 of 2012.

2 Personal Data Protection Commission website <https://www.pdpc.gov.sg/legislation-and-guidelines/overview> (accessed 7 January 2017). The word "organisation" is defined under s 2(1) of the Personal Data Protection Act 2012 (Act 26 of 2012) to include "any individual, company, association or body of persons, corporate or unincorporated, whether or not (*a*) formed or recognised under the law of Singapore; or (*b*) resident, or having an office or a place of business, in Singapore".

enforce, as well as lead to the creation of a trade barrier. Nor does stringency guarantee better protection in every case.[3]

2 This article examines the role and concept of consent under the PDPA. It shows that the PDPA does not – and rightly so – overemphasise the role of consent in personal data protection. The discussion consists of three main parts. First, at a general level, we consider the significance of consent in personal data protection from both theoretical and practical perspectives. Second, we scrutinise the place of "consent" in the structural framework of the PDPA. Finally, we examine recent decisions delivered by the Personal Data Protection Commission ("PDPC") to gain a better understanding of the enforcement of the consent obligation in practice.

II. Theory of consent in personal data protection

3 Consent is a fundamental legal concept. It is a core requirement of many legal activities, such as the formation of contract, the creation of trust and the transfer of rights. Conversely, the lack of consent for certain acts can lead to legal liability. Consent, as a trigger for a legal event, accords respect to individual autonomy. In the context of personal data, consent operates as a mechanism of authorisation.[4] The requirement of an individual's consent confers control on the individual over the use of his personal data by others.

4 Accordingly, consent should play an important role in any personal data protection legislation. Yet, the theory of consent presupposes that the individual is always able to make a voluntary, informed choice. Consent in practice is likely to present a different picture. It has been forcefully argued that "an overemphasis of autonomous authorisation" will lead to an overload of consent transactions[5] with the consequence that consumers suffer from "consent fatigue" and "consent desensitisation", thereby ultimately weakening the consent mechanism as an effective way of seeking

3 See Bart Willem Schermer *et al*, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection" (2014) 16 *Ethics and Information Technology* 171.

4 See Bart Willem Schermer *et al*, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection" (2014) 16 *Ethics and Information Technology* 171 at 174–175.

5 This problem is particularly acute in the context of Internet activities.

voluntary, intentional and informed authorisation.[6] Alternative models have thus been proposed, including paternalism (banning certain kinds of dealings with personal data); making privacy notices more reasonable and accessible to ensure informed and voluntary choices;[7] and a differentiated consent model where the type of consent required is based on the severity of risks/dangers associated with the particular kind of transaction.[8]

5 Further, the role (and degree of emphasis) of consent within the regulatory framework should be assessed by considering the other interests that are worth protecting. An overemphasis on consent in personal data protection law would undoubtedly lead to higher compliance costs for businesses and slower transaction rates. These consequences would affect both organisations as well as individuals. Beyond purely economic consequences, organisations may require an individual's personal data for legitimate and/or reasonable activities. To accord full control to individuals in deciding whether their personal data may be collected, used or disclosed can have serious impact upon the functioning of social and legal relationships.

6 Next, we turn to examine the role and concept of consent under the PDPA. The analysis shows that the Singapore protection model does not overly emphasise consent. Instead, it embodies a balancing approach that incorporates principles of necessity, reasonableness and fairness.

---

6 Bart Willem Schermer *et al*, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection" (2014) 16 *Ethics and Information Technology* 171 at 176–179.

7 Aleecia M McDonald & Tom Lowenthal, "Nano-notice: Privacy Disclosure at a Mobile Scale" (2013) 3 *Journal of Information Policy* 331.

8 Bart Willem Schermer *et al*, "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection" (2014) 16 *Ethics and Information Technology* 171.

III. Role and concept of consent under the Personal Data Protection Act

A. Concept of consent

7 As a general rule, the PDPA prescribes that an organisation requires consent from the individual to collect, use or disclose personal data relating to that individual. Section 13 of the PDPA provides as follows:

> An organisation shall not, on or after the appointed day, collect, use or disclose personal data about an individual unless —
>
> (*a*) the individual *gives, or is deemed to have given, his consent* under this Act to the collection, use or disclosure, as the case may be; or
>
> (*b*) the collection, use or disclosure, as the case may be, without the consent of the individual is *required or authorised under this Act or any other written law*.
>
> [emphasis added]

8 Relevantly, the meaning of "consent" is not defined in the PDPA. This may raise concerns of uncertainty. However, there is ample guidance under the PDPA when one turns to look at other provisions. Valid consent can only be obtained from an individual, as a general rule, if the individual has been notified of the purposes for the collection, use or disclosure pursuant to s 20.[9] Section 14 provides that consent that is obtained pursuant to deceptive or misleading practices is invalid. Clearly, both s 14 and s 20 are inserted to ensure that consent is given on an *informed* basis. Another limit, imposed by s 18(2), is that personal data may only be collected, used or disclosed for purposes "that a reasonable person would consider appropriate in the circumstances".[10] Section 11(1) further clarifies that "[i]n meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances". The lack of definition is not always a shortcoming: it affords latitude for deciding on a "case-by-case" basis and enables the PDPA to better respond to future technological advancements.

---

9 See ss 14(1)(*a*) and 18(*b*) of the Personal Data Protection Act 2012 (Act 26 of 2012).

10 This means that appropriateness of purpose is determined objectively.

9 Section 13 also makes clear that consent may be *deemed*. Section 15(1) of the PDPA provides that there is deemed consent by an individual to the collection, use or disclosure of his personal data by an organisation for a purpose if the individual "voluntarily provides the personal data to the organisation for that purpose"[11] or it is *reasonable* that he would do so voluntarily.[12] Section 15(2) continues to provide that if an individual has consented or is deemed to have consented to an organisation disclosing his personal data to another organisation for a particular purpose, the individual is deemed to have consented to the disclosure of the data for that particular purpose by the other (receiving) organisation. Of course, the concept of deemed consent is subject to the limitations imposed by s 18 discussed above, namely, notification of purpose as well as reasonableness of purpose.

10 As a matter of principle, "deemed consent" is not actual consent and may seemingly undercut the control which the PDPA confers upon an individual over the collection, use or disclosure of his personal data. However, in practice, "deemed consent" is a cost-effective means for organisations to obtain authorisation. "Deemed consent" may also benefit the individual in terms of transactional efficiency, as it can reduce consent requests and avoid an overload of consent transactions. Besides, the concept of "deemed consent" is properly circumscribed in the PDPA. Where the individual *voluntarily* supplies personal data to an organisation for a purpose, it is generally fair and reasonable for the individual to be treated as having consented to the collection, use and disclosure of the personal data by the organisation for that purpose. For example, a patient who supplies his personal data to a medical clinic for the purpose of making a medical appointment would be deemed to have consented to the medical clinic's collection or use of his personal data for the purpose of seeking medical treatment.[13] It may even be said that consent could be *inferred* in such circumstances.

11 Greater uncertainty may arise in respect of s 15(1)(*b*) – "it is reasonable that the individual would voluntarily provide the data". But

11 Personal Data Protection Act 2012 (Act 26 of 2012) s 15(1)(*a*).

12 Personal Data Protection Act 2012 (Act 26 of 2012) s 15(1)(*b*).

13 Kah Leng Ter, "Information Management: Towards Consumer Data Protection Legislation in Singapore" (2012) 24 SAcLJ 143 at 163.

individuals need not be overly concerned. First, the burden of proof rests on organisations to show that there is deemed consent. Secondly, whether the individual would have voluntarily provided the personal data is a matter to be assessed objectively. Thirdly, the concept of deemed consent is subject to the s 18 limitations.[14] The clearest example of deemed consent under s 15(1)(*b*) would be where a patient seeks or agrees to a referral by his family doctor to a specialist for further medical treatment. For that purpose, the personal information relating to the individual will need to be disclosed to the specialist clinic and consent for disclosure could be deemed in such circumstances.

12 Finally, s 16 of the PDPA provides that consent (including deemed consent) may be withdrawn.[15] The withdrawal of consent operates prospectively: it does not render the prior collection, use or disclosure of personal data unauthorised. The provision for withdrawal of consent provides further control to the individual to decide how his personal data may be used and such control is particularly crucial in situations of deemed consent.

B. Exceptions

13 Section 13(*b*) provides that the consent of the individual is not required in circumstances where the collection, use or disclosure of personal data is statutorily mandated or authorised. We will focus on statutory authorisation under the PDPA. But before that, it should not be missed that s 4(5) of the PDPA excludes from the scope of Pts III–VI "business contact information"[16] that is not expressly referred to therein. This exclusion is defensible on two grounds. First, business contact information, in most cases, is publicly available information.[17] Secondly, business contact information should not be considered personal data, as it is generated in

14 It is less clear how the notification obligation is to be satisfied in respect of s 15(1)(*b*) of the Personal Data Protection Act 2012 (Act 26 of 2012).

15 Note s 16(4) of the Personal Data Protection Act 2012 (Act 26 of 2012).

16 See the definition under s 2(1) of the Personal Data Protection Act 2012 (Act 26 of 2012).

17 Exempted under para 1(*c*) of the Second Schedule (collection); para 1(*c*) of the Third Schedule (use); and para 1(*d*) of the Fourth Schedule (disclosure) to the Personal Data Protection Act 2012 (Act 26 of 2012).

connection with and for professional objectives. The point of business contact information is to enable others to contact the individual for professional reasons.

14 More significantly, section 17 of the PDPA provides that personal data can be collected, used and disclosed *without consent* in the circumstances set out in the Second Schedule (collection), Third Schedule (use) and Fourth Schedule (disclosure). These exceptions are generally characterised by necessity, reasonableness and/or fairness. Essentially, the PDPA acknowledges that certain forms of socially, morally or legally acceptable uses of personal data do not require the individual's consent.[18] It has been pointed out that some of the exemptions appear to be very wide,[19] for instance, collection *necessary* for "evaluative purposes"[20] and where the personal data is publicly available.[21] It must nevertheless be borne in mind that an effective control of any form of potential statutory excessiveness is the interpretation and application of the PDPA provisions by adjudicating bodies.

IV. Personal Data Protection Commission decisions

15 The PDPC's decisions on alleged breaches of the consent obligation will be examined in this Part. A number of key points may be drawn from the decisions.

18 Some of these exceptions may overlap with the concept of deemed consent. See, *eg*, para 1(*n*) of the Second Schedule to the Personal Data Protection Act 2012 (Act 26 of 2012).

19 Hannah Lim Yee Fen, "The Data Protection Paradigm for the Tort of Privacy in the Age of Big Data" (2015) 27 SAcLJ 789 at 819–820.

20 Personal Data Protection Act 2012 (Act 26 of 2012) Second Schedule, para 1(*f*). Also see para 1(*f*) of the Third Schedule and para 1(*h*) of the Fourth Schedule. See the definition of "evaluative purposes" under s 2(1).

21 Personal Data Protection Act 2012 (Act 26 of 2012) Second Schedule, para 1(*c*); Third Schedule, para 1(*c*); Fourth Schedule, para 1(*d*).

A. Consent

16 The PDPC does not generally object to broadly-worded consent requests[22] or opt-out provisions.[23] The question in each case is whether the relevant provision is effective in seeking consent from the individual in relation to the collection, use or disclosure of his personal data for the relevant purpose. Clear and internally consistent drafting is crucial. In the "absence of clear supporting evidence", the PDPC would, out of prudence, refrain from making a finding of breach.[24]

17 Further, the PDPC does not interpret the concept of "deemed consent" under s 15 widely. In *Universal Travel Corp Pte Ltd*,[25] four passengers sought from the tour agency formal confirmation of cancellation of their flight for the purpose of processing their insurance claims. The tour agency disclosed to each of the four passengers the affected passenger list which contained the four passengers' personal data. The PDPC held that the four passengers could not be deemed to have consented to the disclosure, as each passenger only required his own personal information for the purpose of processing his insurance claim. It was also possible, in the circumstances, for the personal data of the relevant passenger to be released to that passenger alone. Nothing on the facts suggested urgency that would necessitate the dispensation of consent under para 1(*a*) of the Fourth Schedule to the PDPA.

B. Neighbouring obligations

18 The PDPC also emphasised the independence and importance of the "neighbouring obligations"[26] – the notification obligation and the reasonableness of purpose obligation under s 18. The PDPC's approach underscores that the PDPA protection framework is not based solely on consent. In particular, the PDPC said that the reasonableness obligation is "an important aspect of the PDPA as it is effective in addressing excesses in the collection, use or disclosure of personal data" under a broadly-worded

22 See *AIA Singapore Pte Ltd* [2016] SGPDPC 10 at [11]–[12].
23 See *YesTuition Agency* [2016] SGPDPC 5.
24 *AIA Singapore Pte Ltd* [2016] SGPDPC 10 at [12].
25 [2016] SGPDPC 4.
26 *Jump Rope (Singapore)* [2016] SGPDPC 21 at [10].

consent clause.[27] Even if an organisation is not to have breached the consent obligation, it may be guilty of breaching the neighbouring obligations.[28]

19 Interestingly, in *Jump Rope (Singapore)*,[29] the PDPC said that in exceptional circumstances, it may be reasonable for an organisation to disclose personal data of an individual without consent.[30] Such circumstances include the disclosure of personal data of an individual who has been dismissed, blacklisted or undergoing disciplinary proceedings for the purpose of warning others. However, the PDPC said that the organisation must comply with the neighbouring obligations.

C. Exceptions

20 In *My Digital Lock Pte Ltd*,[31] the PDPC considered the "publicly available data", the "necessary for investigations and proceedings" and the "necessary for provision of legal services" exceptions under the Fourth Schedule to the PDPA. In respect of the latter two exceptions, the PDPC stressed that the organisation must show necessity and the disclosure would not be considered necessary for those objectives if there are other ways of achieving the same.[32]

D. Enforcement actions

21 In determining the appropriate enforcement actions to be ordered pursuant to s 29 of the PDPA, the PDPC takes into account a broad range of considerations. The decisions on breach of the consent obligation concerned unauthorised disclosure and the relevant considerations are:

(a) the number of third parties to whom the disclosure has been made;
(b) the period of disclosure;
(c) the amount of personal data disclosed;

27 *AIA Singapore Pte Ltd* [2016] SGPDPC 10 at [18].
28 *AIA Singapore Pte Ltd* [2016] SGPDPC 10 at [19].
29 [2016] SGPDPC 21.
30 *Jump Rope (Singapore)* [2016] SGPDPC 21 at [10]. See also [11] (where notification may be dispensed with).
31 [2016] SGPDPC 20.
32 *My Digital Lock Pte Ltd* [2016] SGPDPC 20 at [21].

(d) the level of sensitivity of the disclosed personal data;
(e) the impact of disclosure upon the individual;
(f) whether the disclosure was caused by wilful or systemic failures of the organisation;
(g) whether the organisation has taken proactive correction procedures; and
(h) whether the organisation has been co-operative in the investigation.

22 In less serious cases,[33] the PDPC issued merely a warning to make clear that breaches of the PDPA are taken seriously. In *Universal Travel Corp Pte Ltd*,[34] the PDPC issued directions for extensive remedial steps to be taken by the organisation for being in breach of s 12 of the PDPA, but it refrained from imposing a fine. In *Chua Yong Boon Justin*,[35] the PDPC imposed a $500 fine on the breaching party on account of the fact that the breach was wilful.[36] However, the PDPC set the fine amount at "the lower end of the spectrum" in view of the fact that the disclosure was limited, one-off, and did not cause a harmful impact on the individual.[37]

V. Conclusion

23 It has been shown in this article that the PDPA, quite rightly, does not overly emphasise the role of consent in personal data protection. It seeks to balance the competing interests of the individual and others who may wish to or require the use of the individual's personal data. It does so through differentiating the type of consent (actual or deemed) that is required based on the risks associated with the transaction and by reference to socially and morally acceptable norms. It also dispenses with the consent requirement in circumstances that are characterised by necessity, reasonableness and/or fairness. Further, the rigours of protection under the

33 See, *eg*, *YesTuition Agency* [2016] SGPDPC 5; *My Digital Lock Pte Ltd* [2016] SGPDPC 20 (also in breach of s 24 of the Personal Data Protection Act 2012 (Act 26 of 2012)) and *Jump Rope (Singapore)* [2016] SGPDPC 21 (also in breach of ss 11 and 20).
34 [2016] SGPDPC 4.
35 [2016] SGPDPC 13.
36 *Chua Yong Boon Justin* [2016] SGPDPC 13 at [19(c)].
37 *Chua Yong Boon Justin* [2016] SGPDPC 13 at [21].

PDPA are not (and cannot be) secured by the consent obligation alone. Other neighbouring obligations, such as the notification and reasonableness of purpose obligations, are also central to the regulatory framework.